# TTP Detail – T1650

## TTP Information

Name: Acquire Access

Description: Adversaries may purchase or otherwise acquire an existing access to a target system or network. A variety of online services and initial access broker networks are available to sell access to previously compromised systems.(Citation: Microsoft Ransomware as a Service)(Citation: CrowdStrike Access Brokers)(Citation: Krebs Access Brokers Fortune 500) In some cases, adversary groups may form partnerships to share compromised systems with each other.(Citation: CISA Karakurt 2022)

Footholds to compromised systems may take a variety of forms, such as access to planted backdoors (e.g., [Web Shell](https://attack.mitre.org/techniques/T1505/003)) or established access via [External Remote Services](https://attack.mitre.org/techniques/T1133). In some cases, access brokers will implant compromised systems with a “load” that can be used to install additional malware for paying customers.(Citation: Microsoft Ransomware as a Service)

By leveraging existing access broker networks rather than developing or obtaining their own initial access capabilities, an adversary can potentially reduce the resources required to gain a foothold on a target network and focus their efforts on later stages of compromise. Adversaries may prioritize acquiring access to systems that have been determined to lack security monitoring or that have high privileges, or systems that belong to organizations in a particular sector.(Citation: Microsoft Ransomware as a Service)(Citation: CrowdStrike Access Brokers)

In some cases, purchasing access to an organization in sectors such as IT contracting, software development, or telecommunications may allow an adversary to compromise additional victims via a [Trusted Relationship](https://attack.mitre.org/techniques/T1199), [Multi-Factor Authentication Interception](https://attack.mitre.org/techniques/T1111), or even [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195).

\*\*Note:\*\* while this technique is distinct from other behaviors such as [Purchase Technical Data](https://attack.mitre.org/techniques/T1597/002) and [Credentials](https://attack.mitre.org/techniques/T1589/001), they may often be used in conjunction (especially where the acquired foothold requires [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: resource-development